Crypto 9/1/2021

Vigenere Idea, How to encrypt/decrypt.

Start talk breaking

Today, Friday - I need to leave a bit early!!!

Plain Text to encrypt: $\overset{6}{G}\overset{14}{O}\ \overset{10}{K}\overset{13}{N}\overset{8}{I}\overset{6}{G}\overset{7}{H}\overset{19}{T}\overset{18}{S}$

$+\ \overset{20}{U}\overset{2}{C}\ \overset{5}{F}\overset{20}{U}\overset{2}{C}\overset{5}{F}\overset{20}{U}\overset{2}{C}\overset{5}{F}$

26, 16, 15, 33, 10, 11, 27, 21, 23 } mod

Key = "UCF"

0, 16, 15, 7, 10, 11, 1, 21, 23

A Q P H K L B V X

3 separate shift ciphers cycled

|k| separate shift ciphers

1. Same letter encrypt into different ciphertext letters
2. Diff plain encrypt into same cipher.

If we "knew" the keylength, then we __WOULD__ know which letters were shifted the same, and hence have partial letter freq info about the plaintext. (Wouldn't have digrams, trigrams, other structular stuff related to consec. letters.)

Repeated substring length 3 or greater

Plain THE
HORSE

THE
HORSE → probability line up 1/5

If we had 6 THE's by pigeonhole principle some 2 of them __must__ line up.
(Prob we have 5 THE none line up
$= \frac{5\times4\times3\times2\times1}{5\times5\times5\times5\times5} = \frac{120}{3125} =$ small)

20 2 5
UCF
7 0 3
HAD

27 2 8
1 2 8
B C I

10 13 8
KNI
17 15
RPA

BCI

Probability of spurious match of diff plain ~~cipher~~ text is LOW

Kasiski Test

Find letter positions of repeated cipher text

QRM: 10, 82, 676

keyword len multiple $82 - 10 = 72$
keyword len multiple $676 - 82 = 594$

$$594 = 8 \times 72 + 18$$
$$72 = 4 \times \boxed{18}$$

$$\begin{array}{r} 594 \\ -576 \\ \hline 8 \end{array}$$

Index of Coincidence

Given a set of items in a single bin (repeated items), if I randomly pull 2 out of the bin, what is the probability they are same?

10 Skittles, 5 M+M, 20 Twix, 15 KitKats

$$p(2\text{ same}) = p(2\,Sk) + p(2\,mm) + p(2T) + p(2K)$$
$$= \frac{10}{50} \times \frac{9}{49} + \frac{5}{50} \times \frac{4}{49} + \frac{20}{50} \times \frac{19}{49} + \frac{15}{50} \times \frac{14}{49}$$

$$= \frac{90+20+380+210}{2450} = \frac{70}{245} = \frac{14}{49} = \boxed{\frac{2}{7}}$$

4

$$IC = \sum_{i=1}^{k} \frac{f_i(f_i-1)}{n(n-1)}$$

$$\boxed{\sum_{i=1}^{k} f_i = n}$$ total # objects

Pretend our candies are English letters :)

8% A, 12% E, .1% Z, etc.

IC(English) ~ .0676 6.76%

IC(Random letters) ~ $\frac{1}{26}$ ~ 3.8ish %

1. Guess a keyword length
2. Separate out bins of ciphertext letters
3. Calc IC for each bin

index array
freq array
MOD